CLAIMS

What is claimed is:

1. A digital rights management system for use in an industrial environment comprising:

a certification component that generates certificates for local domain automation devices; and

an access component that establishes rules of use for automation device services based at least upon the identity of a user or entity as provided by a certificate.

2. The system of claim 1, wherein the system is executed by a computer remotely located from the automation device.

3. The system of claim 2, wherein communication between the automation device and the certification and access components is over a local area network.

4. The system of claim 3, wherein communication is secured *via* digital certificates which bind public keys to specific users and/or entities to facilitate decryption of a message as well as identification of a sender.

5. The system of claim 4, wherein the message is digitally signed to enable the message to be authenticated.

6. The system of claim 1, wherein access to the access component is a restricted component limited to a particular user or group of users *via* certificates.

7. The system of claim 1, wherein the automation device includes an access credential component that defines and restricts access to particular objects and services based on the identity of the user as established by a certificate.

8. The system of claim 7, wherein the automation device includes a virtual key component adapted to retrieve identifying information from a certificate.

9. The system of claim 7, wherein the access credential component also defines and restricts access based on a personal id provided by a SIM card.

10. The system of claim 9, wherein the automation device includes a physical key component adapted to retrieve identifying information from the SIM card.

11. The system of claim 1, wherein the automation device is one of a programmable logic controller, an I/O device, and a communication adaptor.

12. A secure automation device communication system comprising:

a certification component; and

a plurality of automation devices that interact with the certification component to generate and receive certificates which bind public keys to specific automation devices to facilitate identification of the devices that generate encrypted messages.

13. The system of claim 12, wherein the automation devices include programmable logic controllers, I/O devices, and communication adapters.

14. The system of claim 12, wherein the automation devices communicate messages over a local area network.

15. The system of claim 12, wherein certificates contain an automation device or user name or ID and a public key associated therewith.

16. The system of claim 12, wherein the certification component stores certificates in a certificate data store isolated from automation devices.

17. The system of claim 12, wherein automation devices contain private keys to facilitate encryption and/or decryption of messages.

18. The system of claim 12, wherein a first automation device utilizes one key in a public private key pair to create a secure message component that is transmitted to a second automation device.

19. The system of claim 18, wherein the second automation device receives the secure message component and utilizes the other key in a public private key pair to decrypt the message component.

20. The system of claim 12, wherein messages are digitally signed and include a message, message digest, and information regarding a hash algorithm.

21. The system of claim 20, wherein the hash algorithm is MD5.

22. A method of managing digital rights comprising:
defining rules of use concerning automation device program privileges;
downloading the rules to an automation device;
limiting interaction with the automation device based on the rules and an identity of a user.

23. The method of claim 22, wherein user identity is established *via* digital certificates.

24. The method of claim 23, wherein user digital certificates are generated by a local area control component.

25. The method of claim 23, wherein the user identity is established utilizing a SIM card.

26. The method of claim 23, wherein user identity is established employing biometrics.

27. The method of claim 22, wherein user rules prohibit particular users from viewing portions of an automation device program.

28. The method of claim 22, wherein user rules prohibit particular users from modifying a ladder logic program.

29. A computer readable medium having stored thereon computer executable instructions for carrying out the method of claim 22.

30. An industrial automation device communication methodology comprising:

encrypting a message to be sent to a automation device utilizing a key; and

transmitting the encrypted message to the automation device.

31. The methodology of claim 30 further comprising:

receiving an encrypted message from an automation device or device controller;

locating a certificate component associated with the automation device sending the message; and

decrypting the message utilizing the public key provided by the certificate component.

32. The method of claim 31, wherein the automation device is an industrial programmable logic controller (PLC).

33. The method of claim 32, wherein the message is a PLC program.

34. The method of claim 31, wherein locating the certificate component comprises searching local automation device store.

35. The method of claim 31, wherein locating the certificate comprises downloading the certificate from a certification component.

36. A computer readable medium having stored thereon computer executable instructions for carrying out the method of claim 31.

37. A method of industrial automation device communication comprising:

generating a digitally signed message component comprising a message, a message digest, and hash function data, wherein the message component is generated by a first industrial automation device; and

transmitting the message component to a second industrial automation device.

38. The method of claim 37, further comprising encrypting the message component prior to transmission.

39. The method of claim 38, further comprising receiving and decrypting the message component.

40. The method of claim 37, further comprising authenticating the message by retrieving a hash function in accordance with the hash information, generating a message digest by applying the retrieved hash function to the received message and comparing the generated message digest with the message digest retrieved from the message component.

41. A computer readable medium having stored thereon computer executable instructions for carrying out the method of claim 37.